UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,070	08/30/2006	Noriyoshi Tsuyuzaki	OKB-017	5909

20374   7590   08/21/2009
KUBOVCIK & KUBOVCIK
SUITE 1105
1215 SOUTH CLARK STREET
ARLINGTON, VA 22202

EXAMINER
YANG, JAMES J

ART UNIT	PAPER NUMBER
4147	

MAIL DATE	DELIVERY MODE
08/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/591,070	Applicant(s) TSUYUZAKI, NORIYOSHI
	Examiner JAMES YANG	Art Unit 4147

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>30 August 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-19</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-19</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>30 August 2006</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>08/30/2006</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385.

Claim 18 claims "An authentication program…" However, the claims do not define a computer-readable program to be a functional descriptive material encoded on a memory/disk, see Applicant's specification, Page 19, Lines 1-11, and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized"). Moreover, "An authentication program" is neither a process ("action", i.e., transform underlying claimed subject matter to a different state or thing), nor machine (not tied to another statutory class, such as a particular apparatus), nor manufacture, nor composition of matter (i.e., tangible "thing") and therefore non-statutory.

Because the full scope of the claim as properly read in light of the

disclosure encompasses non-statutory subject matter, the claim as a whole is

non-statutory and appears to be one type of claim that is considered

nonstatutory, under the present USPTO Interim Guidelines, 1300 Official Gazette

Patent and Trademark Office 142 (Nov. 22, 2005).

Claim 19 is further rejected under 35 U.S.C. 101 because of its

dependency on a rejected claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claims 6 and 13 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as the invention.

Regarding claims 6 and 13, the phrase "or the like" renders the claim(s)

indefinite because the claim(s) include(s) elements not actually disclosed (those

encompassed by "or the like"), thereby rendering the scope of the claim(s)

unascertainable. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1.   Claims 1-4, 8, 9-11, and 15-19 are rejected under 35 U.S.C. 102(b) as

being anticipated by Shi (EP 0957220).

Claim 1, Shi teaches:

An authentication apparatus comprising

a body, and a partner side paired with the body (*Shi,* Paragraph

[0008]: "The cryptogram lock system with automatically variable true random

code comprises *a lock-body and a key-body* with a bi-directional communication

link established therebetween (either through connecting wire or radio set)." The

lock body is a *body,* and the key-body is a *partner side.*), the apparatus

comprising:

a random pulse generator, arranged in the body or the partner side,

or in both the body and the partner side (*Shi,* Paragraph [0008]: "The lock-

body comprises a lock mechanism portion and a control portion, wherein said

control portion comprises a microprocessor IC1, a non-volatile memory unit IC2,

a *true random code generator IC3,* and an output driver IC5 for driving said lock

mechanism portion, and an alarm unit IC6." The random code generator IC3 is a

random pulse generator, and is arranged in the body.), **which generates**

random pulses (*Shi*, Paragraph [0009]: "Whenever the cryptogram lock is

opened successfully, the microprocessor IC1 takes out immediately *a new code*

from the true random code generator to replace the previous one stored in the

memory units IC2 and IC4 so as to make the lock system ready for the next

operation." The random pulse generation is disclosed in Fig. 3 and Paragraph

[0017].);

  a means which outputs authentication data based on the random

pulses generated by the random pulse generator (*Shi*, Paragraph [0013]:

"Whenever the lock is opened successfully, the *microprocessor IC1 takes out*

automatically a new code from the true random code generator and stored it

simultaneously in the memory units IC2 and IC4, respectively, for the next

opening operation." The microprocessor IC1 outputs the new codes from the

code generator and stores them in memory units.);

  a means which stores authentication data (*Shi*, Paragraph [0006]: "In

addition, the code *stored in the memory units* of the lock-body as well as the key-

body is not a permanent one, but one automatically changed every time after the

lock is opened successfully."),

  a communication means which transmits/receives authentication

data (*Shi*, Paragraph [0008]: "The cryptogram lock system with automatically

variable true random code comprises a lock-body and a key-body with a bi-

directional *communication link established therebetween* (*either through*

connecting wire or radio set)."); and

a control means which controls the communication of authentication data and collates authentication data (*Shi*, Paragraph [0009]: "When a communication link is established between the lock-body and the key-body, *the microprocessor IC1* within the lock-body takes out the code stored in the memory of the IC4 of the key-body and compares it with the code stored in the unit IC2 of the lock-body." Microprocessor IC1 is the *control means*, and the comparison between the codes stored in the lock-body and the key-body is the *collation of the authentication data*.).

Claim 2, Shi further teaches:

The control means receives authentication data stored in the storage means arranged on the partner side, collates the received authentication data with authentication data of the storage means arranged in the body (*Shi*, Paragraph [0009]: "When a communication link is established between the lock-body and the key-body, *the microprocessor IC1* within the lock-body takes out the code stored in the memory of the IC4 of the key-body and compares it with the code stored in the unit IC2 of the lock-body." Microprocessor IC1 is the *control means*, and the comparison between the codes stored in the lock-body and the key-body is the *collation of the authentication data*.), **and in accordance with the result of collation, authenticates the partner side** (*Shi*, Paragraph [0009]: "*If the two codes are coincident with each other*, the microprocessor controls the driving mechanism to open the lock, otherwise the microprocessor activates the alarm unit to send out an alarm signal."), **and in that upon**

completion of the authentication, authentication data is updated, and new

authentication data thus updated is written in the storage means of the

body and the partner side (Shi, Paragraph [0009]: "Whenever the cryptogram

lock is opened successfully, the microprocessor IC1 takes out immediately *a new*

code from the true random code generator to replace the previous one stored in

the memory units IC2 and IC4 so as to make the lock system ready for the next

operation.").

Claim 3, *Shi further teaches:*

A drive unit control means which controls a drive unit in accordance

with the result of collation by the control means (*Shi*, Paragraph [0009]: "*If*

the two codes are coincident with each other, the *microprocessor controls the*

driving mechanism to open the lock, otherwise the microprocessor activates the

alarm unit to send out an alarm signal." The driving mechanism, represented by

an output drive IC5, is a *drive unit control means,* which controls the lock of a

lock-body, which is a *drive unit.*).

Claim 4, *Shi further teaches:*

The body is the body of an electronic lock, and the partner side is a

key (*Shi*, Paragraph [0008]: "The *lock-body* comprises a lock mechanism portion

and a control portion, wherein said control portion comprises a microprocessor

IC1, a non-volatile memory unit IC2, a true random code generator IC3, and an

output driver IC5 for driving said lock mechanism portion, and an alarm unit IC6.

Said *key-body* further comprises a non-volatile memory unit IC4." The lock-body

comprises a microprocessor, memory, random code generator, driver, and alarm

unit, thus it is an electronic lock.).

Claim 8, *Shi further teaches:*

The communication means transmits/receives the authentication

data by circuit connection due to contact or by infrared light

communication or radio communication (*Shi*, Paragraph [0008]: "The

cryptogram lock system with automatically variable true random code comprises

a lock-body and a key-body with a bi-directional *communication link established*

therebetween (*either through connecting wire or radio set*).").

Claim 9, Shi teaches:

An authentication method comprising the steps of:

generating random pulses by a random pulse generator (*Shi*,

Paragraph [0009]: "Whenever the cryptogram lock is opened successfully, the

microprocessor IC1 takes out immediately *a new code from the true random*

code generator to replace the previous one stored in the memory units IC2 and

IC4 so as to make the lock system ready for the next operation." The random

pulse generation is disclosed in Fig. 3 and Paragraph [0017].) **arranged in a**

body or a partner side paired with the body, or in both the body and the

partner side (*Shi*, Paragraph [0008]: "The lock-body comprises a lock

mechanism portion and a control portion, wherein said control portion comprises

a microprocessor IC1, a non-volatile memory unit IC2, a *true random code generator IC3*, and an output driver IC5 for driving said lock mechanism portion, and an alarm unit IC6." The random code generator IC3 is a *random pulse generator*, and is arranged in the body.**);**

outputting authentication data based on the random pulses generated by the random pulse generator (*Shi***, Paragraph [0013]: "Whenever the lock is opened successfully, the *microprocessor IC1 takes out automatically a new code from the true random code generator* and stored it simultaneously in the memory units IC2 and IC4, respectively, for the next opening operation." The microprocessor IC1 outputs the new codes from the code generator and stores them in memory units.);**

storing authentication data (*Shi***, Paragraph [0006]: "In addition, the code *stored in the memory units* of the lock-body as well as the key-body is not a permanent one, but one automatically changed every time after the lock is opened successfully.");**

transmitting/receiving authentication data (*Shi***, Paragraph [0008]: "The cryptogram lock system with automatically variable true random code comprises a lock-body and a key-body with a bi-directional *communication link established therebetween (either through connecting wire or radio set).");* and**

controlling the communication of authentication data and collating authentication data (*Shi***, Paragraph [0009]: "When a communication link is established between the lock-body and the key-body, *the microprocessor IC1* within the lock-body takes out the code stored in the memory of the IC4 of the**

key-body and compares it with the code stored in the unit IC2 of the lock-body."

Microprocessor IC1 is the *control means*, and the comparison between the codes

stored in the lock-body and the key-body is the *collation of the authentication*

data.).

       Claim 10, Shi further teaches:

       The control step receives the authentication data stored in a storage

means arranged on the partner side, collates the received authentication

data with authentication data of a storage means arranged in the body (*Shi*,

Paragraph [0009]: "When a communication link is established between the lock-

body and the key-body, *the microprocessor IC1* within the lock-body takes out

the code stored in the memory of the IC4 of the key-body and compares it with

the code stored in the unit IC2 of the lock-body." Microprocessor IC1 is the

control means, and the comparison between the codes stored in the lock-body

and the key-body is the *collation of the authentication data*.), **authenticates the**

partner side in accordance with the result of collation (*Shi*, Paragraph

[0009]: "*If the two codes are coincident with each other*, the microprocessor

controls the driving mechanism to open the lock, otherwise the microprocessor

activates the alarm unit to send out an alarm signal."), **and after completion of**

authentication, updates authentication data, and writes new authentication

data thus updated in the storage means of the body and the partner side

(Shi, Paragraph [0009]: "Whenever the cryptogram lock is opened successfully,

the microprocessor IC1 takes out immediately *a new code from the true random*

code generator to replace the previous one stored in the memory units IC2 and

IC4 so as to make the lock system ready for the next operation.").

Claim 11, Shi further teaches:

A drive unit control step for controlling a drive unit in accordance

with the result of collation in the control step (*Shi*, Paragraph [0009]: "*If the*

two codes are coincident with each other, the *microprocessor controls the driving*

mechanism to open the lock, otherwise the microprocessor activates the alarm

unit to send out an alarm signal." The driving mechanism, represented by an

output drive IC5, is a *drive unit control means,* which controls the lock of a lock-

body, which is a *drive unit.*).

Claim 15, *Shi further teaches:*

The communication step transmits and receives the authentication

data by circuit connection due to contact or by infrared light

communication or radio communication (*Shi*, Paragraph [0008]: "The

cryptogram lock system with automatically variable true random code comprises

a lock-body and a key-body with a bi-directional *communication link established*

therebetween (*either through connecting wire or radio set*).").

Claim 16, Shi further teaches:

The body or the partner side includes the hardware of a computer

(*Shi*, Paragraph [0012]: "The control portion in the lock-body comprises a

microprocessor IC1, a non-volatile memory unit IC2 and a true random code

generator IC3." The microprocessor IC1 and the non-volatile memory unit IC2

are *hardware of a computer*, and the body includes the hardware.), **and the**

partner side or the body including the random pulse generator is mounted

integrally with or independently of the hardware of the computer (*Shi*,

Paragraph [0012]: "The control portion in the lock-body comprises a

microprocessor IC1, a non-volatile memory unit IC2 and *a true random code*

generator IC3." As further disclosed in Fig. 1, the true random generator IC3 is

mounted integrally with the hardware of the computer components IC1 and IC2

within the lock-body.).

Claim 17, *Shi further teaches:*

The body or the partner side includes the hardware of a computer

(*Shi*, Paragraph [0012]: "The control portion in the lock-body comprises a

microprocessor IC1, a non-volatile memory unit IC2 and a true random code

generator IC3." The microprocessor IC1 and the non-volatile memory unit IC2

are *hardware of a computer*, and the body includes the hardware.), **and the**

partner side or the body including the random pulse generator is mounted

integrally with or independently of the hardware of the computer (*Shi*,

Paragraph [0012]: "The control portion in the lock-body comprises a

microprocessor IC1, a non-volatile memory unit IC2 and *a true random code*

generator IC3." As further disclosed in Fig. 1, the true random generator IC3 is

mounted integrally with the hardware of the computer components IC1 and IC2
within the lock-body.).

Claim 18, Shi teaches:

An authentication program (*Shi*, Paragraph [0006]: "In addition, the
code stored in the memory units of the lock-body as well as the key-body is not a
permanent one, but one *automatically* changed every time the lock is opened
successfully." Shi discloses in Fig. 2 a flow chart showing the operation of the
cryptogram lock system performed by the microprocessor IC1, non-volatile
memory unit of the lock-body and key-body, random code generator IC3, output
driver IC5, and alarm unit IC6, which is automatically performed. It is inherent of
a system that automatically performs the steps disclosed in Fig. 2 and Paragraph
[0020] that the steps, as a whole, are programmed into the microprocessor IC1 of
the lock-body.) **comprising:**

a code to generate random pulses from a random pulse generator
(*Shi*, Paragraph [0009]: "Whenever the cryptogram lock is opened successfully,
the microprocessor IC1 takes out immediately *a new code from the true random
code generator* to replace the previous one stored in the memory units IC2 and
IC4 so as to make the lock system ready for the next operation." The random
pulse generation is disclosed in Fig. 3 and Paragraph [0017].) **arranged in a
body or a partner side paired with the body, or in both the body and the
partner side partner side** (*Shi*, Paragraph [0009]: "Whenever the cryptogram
lock is opened successfully, the microprocessor IC1 takes out immediately *a new*

code from the true random code generator to replace the previous one stored in

the memory units IC2 and IC4 so as to make the lock system ready for the next

operation." The random pulse generation is disclosed in Fig. 3 and Paragraph

[0017].);

a code to output authentication data based on the random pulses

generated by the random pulse generator (*Shi*, Paragraph [0013]: "Whenever

the lock is opened successfully, the *microprocessor IC1 takes out automatically a*

new code from the true random code generator and stored it simultaneously in

the memory units IC2 and IC4, respectively, for the next opening operation." The

microprocessor IC1 outputs the new codes from the code generator and stores

them in memory units.**)**;

a code to store authentication data (*Shi*, Paragraph [0006]: "In addition,

the code *stored in the memory units* of the lock-body as well as the key-body is

not a permanent one, but one automatically changed every time after the lock is

opened successfully."**)**;

a code to transmit/receive authentication data (*Shi*, Paragraph [0008]:

"The cryptogram lock system with automatically variable true random code

comprises a lock-body and a key-body with a bi-directional *communication link*

established therebetween (*either through connecting wire or radio set*)."**); and**

a code to control the communication of authentication data and

collate authentication data (*Shi*, Paragraph [0009]: "When a communication

link is established between the lock-body and the key-body, *the microprocessor*

IC1 within the lock-body takes out the code stored in the memory of the IC4 of

the key-body and compares it with the code stored in the unit IC2 of the lock-body." Microprocessor IC1 is the *control means*, and the comparison between the codes stored in the lock-body and the key-body is the *collation of the authentication data*.).

Claim 19, Shi further teaches:

The code to control the communication of authentication data and collate authentication data includes: a code to receive authentication data stored in a storage means arranged on the partner side (*Shi***, Paragraph [0009]: "When a communication link is established between the lock-body and the key-body, *the microprocessor IC1* within the lock-body *takes out the code stored in the memory of the IC4 of the key-body* and compares it with the code stored in the unit IC2 of the lock-body." The memory of the IC4 of the key-body is the *storage means arranged on the partner side*.); a code to collate the received authentication data with authentication data of a storage means arranged in the body (***Shi***, Paragraph [0009]: "When a communication link is established between the lock-body and the key-body, *the microprocessor IC1* within the lock-body takes out the code stored in the memory of the IC4 of the key-body and compares it with the code stored in the unit IC2 of the lock-body."** Microprocessor IC1 is the *control means*, and the comparison between the codes stored in the lock-body and the key-body is the *collation of the authentication data*.**); a code to authenticate the partner side in accordance with the result of collation (***Shi***, Paragraph [0009]: "*If the two codes are coincident with each*

other, the microprocessor controls the driving mechanism to open the lock,

otherwise the microprocessor activates the alarm unit to send out an alarm

signal."**); a code to update authentication data after completion of the**

authentication (Shi, Paragraph [0009]: "Whenever the cryptogram lock is

opened successfully, the microprocessor IC1 takes out immediately *a new code*

from the true random code generator to replace the previous one stored in the

memory units IC2 and IC4 so as to make the lock system ready for the next

operation."**); and a code to write new authentication data thus updated in the**

storage means of the body and the partner side (Shi, Paragraph [0009]:

"Whenever the cryptogram lock is opened successfully, the microprocessor IC1

takes out immediately *a new code from the true random code generator to*

replace the previous one stored in the memory units IC2 and IC4 so as to make

the lock system ready for the next operation."**).**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

2.   Claims 5, 7, 12, and 14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Shi (EP 0957220) in view of Shilton (WO 99/41834).

Claim 5, Shi does not teach:

The random pulse generator detects the α particles, the beta ray or the gamma ray released by the collapse of the atomic nucleus and generates random pulses.

Shilton teaches:

The random pulse generator detects the α particles, the beta ray or the gamma ray released by the collapse of the atomic nucleus (*Shilton,*** Page 5, Lines 18-20: "The basic design concept of the RPG consists of a low activity radiation source which emits alpha, beta, gamma, X ray, conversion electron, auger electron or other random radiation emissions arising from ***radioactive decay.***" The radiation is detected by a PIN diode (see Shilton, Page 5, Lines 30-31) or directly onto a silicon chip (see Shilton, Page 6, Lines 1-2). The radioactive decay is the ***collapse of the atomic nucleus.***) and generates random pulses (***Shilton,*** Page 4, Lines 13-15: "The combined source and detector in the form of an RPG, produces random voltage and/or current pulses.").**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the random code generator in Shi by integrating the low radiation source and detector for generating random events as taught by Shilton.

The motivation would be to produce random codes that are difficult to duplicate to prevent fraud or corruption of random pulse generators (see Shilton, Page 1, Lines 9-18).

Claim 7, Shi in view of Shilton teaches:

The random pulse generator detects thermal electrons, noises or jitters or receives a radio wave (RF) (*Shilton***, Page 5, Lines 30-31: "Such a** source is placed in close proximity to a suitable *radiation detector* which can be a simple PIN diode comprising a small other solid state semiconductor detector. Alternatively radioactivity can be deposited directly onto a silicon chip which can act as the substrate. When a bias voltage is applied to the silicon detector, alpha particles which are emitted by the source into the silicon detector produce a voltage and/or current pulse." The detector can detect the number of pulses produced in a given time interval, and thus can detect jitters (see Shilton, Page 6, Lines 16-25).**) and generates random pulses (***Shilton***, Page 4, Lines 13-15:** "The combined source and detector in the form of an RPG, produces random voltage and/or current pulses.")**.**

Claim 12, *Shi does not teach:*

The random pulse generator detects the α particles, the beta ray or the gamma ray released by the collapse of the atomic nucleus and generates random pulses.

Shilton teaches:

The random pulse generator detects the α particles, the beta ray or the gamma ray released by the collapse of the atomic nucleus (*Shilton,*** Page 5, Lines 18-20: "The basic design concept of the RPG consists of a low activity radiation source which emits alpha, beta, gamma, X ray, conversion electron, auger electron or other random radiation emissions arising from radioactive decay." The radiation is detected by a PIN diode (see Shilton, Page 5, Lines 30-31) or directly onto a silicon chip (see Shilton, Page 6, Lines 1-2).) and generates random pulses (***Shilton,*** Page 4, Lines 13-15: "The combined source and detector in the form of an RPG, produces random voltage and/or current pulses.").**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the random code generator in Shi by integrating the low radiation source and detector for generating random events as taught by Shilton.

The motivation would be to produce random codes that are difficult to duplicate to prevent fraud or corruption of random pulse generators (see Shilton, Page 1, Lines 9-18).

Claim 14, *Shi in view of Shilton teaches:*

The random pulse generator detects thermal electrons, noises or jitters or receives a radio wave (RF) (*Shilton***, Page 5, Lines 30-31: "Such a** source is placed in close proximity to a suitable *radiation detector* which can be a simple PIN diode comprising a small other solid state semiconductor detector. Alternatively radioactivity can be deposited directly onto a silicon chip which can act as the substrate. When a bias voltage is applied to the silicon detector, alpha particles which are emitted by the source into the silicon detector produce a voltage and/or current pulse." The detector can detect the number of pulses produced in a given time interval, and thus can detect jitters (see Shilton, Page 6, Lines 16-25).**) and generates random pulses (***Shilton***, Page 4, Lines 13-15:** "The combined source and detector in the form of an RPG, produces random voltage and/or current pulses.")**.

3.   Claims 6 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shi (EP 0957220) in view of Shilton (WO 99/41834), and further in view of Barker (U.S. 5,076,971).

Claim 6, Shi in view of Shilton teach:

^{241}Am, ^{210}Pb-^{210}Po, ^{210}Po, ^{244}Cm, or the like is used as an α particle radiator (*Shilton***, Page 5, Lines 21-25: "The preferred emissions are** substantially mono-energetic alpha particles or conversion electrons, more preferably alpha particles from a radionuclide with a long half-life, for example

upwards of 140 days such as ^{241}Am, ^{252}Cf, ^{250}Cf, ^{226}Ra, ^{238}U, ^{244}Cm, ^{243}Cm,

^{228}Th, ^{208}Po, ^{209}Po, ^{210}Po, ^{238}Pu or ^{148}Gd or a combination of these.").

Shi in view of Shilton teach:

^{210}Pb, or the like as a beta ray radiator.

Barker teaches:

^{210}Pb, or the like as a beta ray radiator (*Barker,*** Col. 9, Lines 9-11: "The**

chain proceeds to Pb 210, which decays by alpha and beta emission with a half-

life of 21 years.").

Therefore, it would have been obvious to one of ordinary skill in the art at

the time of the invention to modify the radiation source in Shi in view of Shilton

with a ^{210}Pb beta emitter as taught by Barker.

The motivation would be to provide a stable beta radiation source with a

long half-life (see Barker, Col. 2, Lines 6-16) applicable as a low activity radiation

source in a Random Pulse Generator (see Shilton, Page 5, Lines 18-30).

Claim 13, *Shi in view of Shilton teach:*

^{241}Am, ^{210}Pb-^{210}Po, ^{210}Po, ^{244}Cm, or the like is used as an α particle

radiator (*Shilton,*** Page 5, Lines 21-25: "The preferred emissions are**

substantially mono-energetic alpha particles or conversion electrons, more

preferably alpha particles from a radionuclide with a long half-life, for example upwards of 140 days such as ^{241}Am, ^{252}Cf, ^{250}Cf, ^{226}Ra, ^{238}U, ^{244}Cm, ^{243}Cm, ^{228}Th, ^{208}Po, ^{209}Po, ^{210}Po, ^{238}Pu or ^{148}Gd or a combination of these.").

Shin in view of Shilton does not teach:

^{210}Pb, or the like as a beta ray radiator.

Barker teaches:

^{210}Pb, or the like as a beta ray radiator (*Barker***, Col. 9, Lines 9-11: "The chain proceeds to Pb 210, which decays by alpha and beta emission with a half-life of 21 years.").**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the radiation source in Shi in view of Shilton with a ^{210}Pb beta emitter as taught by Barker.

The motivation would be to provide a stable beta radiation source with a long half-life (see Barker, Col. 2, Lines 6-16) applicable as a low activity radiation source in a Random Pulse Generator (see Shilton, Page 5, Lines 18-30).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES YANG whose telephone number is (571)270-5170. The examiner can normally be reached on M-F 7:30-5 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hai Tran can be reached on 5712727305. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.Y./

/GEORGE BUGG/
Primary Examiner, Art Unit 4147